

Oracle® Storage 12Gb/s SAS PCIe RAID HBA, 내부 보안 설명서

HBA 모델 7110116 및 7110117



부품 번호: E59790-01
2014년 12월

Copyright © 2014, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 계약서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 계약서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제 3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제 3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다.

목차

Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부 보안	5
HBA 개요	5
보안 원칙	6
보안 환경 계획	7
하드웨어 보안	7
소프트웨어 보안	7
펌웨어 보안	8
Oracle ILOM 펌웨어	8
시스템 로그	8
보안 환경 유지 관리	8
자산 추적	9
펌웨어 업데이트	9
소프트웨어 업데이트	9
로그 보안	10
모듈 보안	10

Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부 보안

이 문서는 Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부를 사용할 때 고려해야 할 기본 보안 원칙 및 지침을 제공합니다.

이 설명서에서는 다음 보안 정보를 다루지 않습니다.

- BIOS, OBP(Open Boot Prom) 및 Hypervisor와 관련된 특정 플랫폼 펌웨어 보안
- 운영 체제 보안 문제
- 하드웨어 시스템의 물리적인 보안
- 외부 네트워킹 기반구조의 네트워크 보안
- TPM(Trusted Platform Module) 정보

이러한 보안 영역에 대한 보안 정보는 해당 제품과 함께 제공된 보안 설명서를 참조하십시오.

이 문서는 다음 항목으로 구성됩니다.

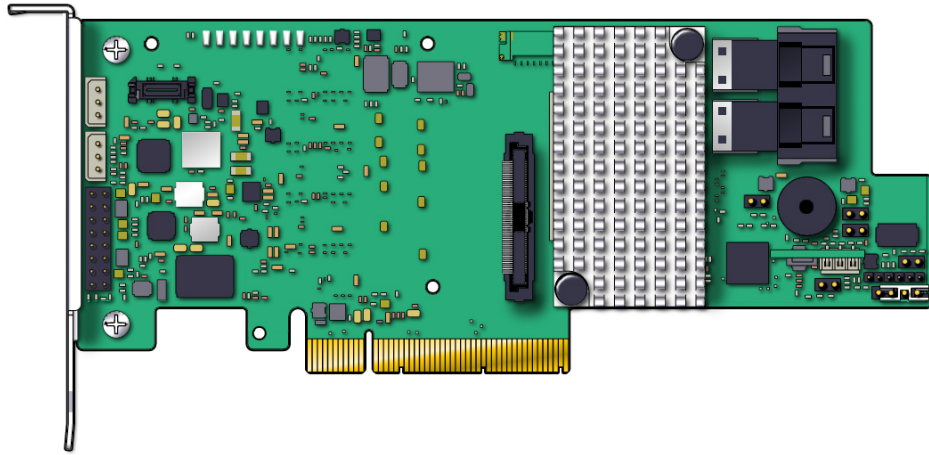
- [“HBA 개요” \[5\]](#)
- [“보안 원칙” \[6\]](#)
- [“보안 환경 계획” \[7\]](#)
- [“보안 환경 유지 관리” \[8\]](#)

HBA 개요

Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부(마케팅 부품 번호 7110116 및 7110117)는 PCIe 3.0 로우 프로파일 RAID 컨트롤러로서, 2개의 SFF-8643 x4 내부 미니 SAS HD 커넥터를 통해 8개의 내부 12Gb/s SAS/SATA 포트를 지원합니다.

참고 - SATA II는 이 HBA에서 유일하게 지원하는 SATA 유형입니다.

다음 이미지는 Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부를 보여줍니다.



보안 원칙

액세스, 인증, 권한 부여 및 계정 관리의 네 가지 기본 보안 원칙이 있습니다.

■ 액세스

물리적 제어 및 소프트웨어 제어를 통해 침입으로부터 하드웨어 또는 데이터를 보호합니다.

- 하드웨어의 경우 액세스 제한은 일반적으로 물리적 액세스 제한을 의미합니다.
- 소프트웨어의 경우 액세스는 물리적 수단 및 가상 수단을 통해 제한됩니다.
- 펌웨어는 Oracle 업데이트 프로세스를 통해서만 변경할 수 있습니다.

■ 인증

사용자가 실제로 등록된 사용자인지 확인할 수 있도록 사용 중인 플랫폼 운영 체제에서 암호 시스템 등의 인증 기능을 설정합니다.

담당자가 컴퓨터실에 출입할 때는 사원 명찰을 사용하도록 합니다.

■ 권한 부여

담당자가 사용 교육 및 자격을 받은 하드웨어와 소프트웨어만 사용할 수 있도록 합니다. 읽기/쓰기/실행 권한 시스템을 설정하여 명령, 디스크 공간, 장치 및 응용 프로그램에 대한 사용자 액세스 권한을 제어합니다.

■ 계정 관리

Oracle 소프트웨어 및 하드웨어 기능을 사용하여 로그인 작동을 모니터링하고 하드웨어 인벤토리를 유지 관리합니다.

- 시스템 로그를 사용하여 사용자 로그인을 모니터링합니다. 특히 시스템 관리자 및 서비스 계정은 강력한 명령에 액세스할 수 있으므로 반드시 모니터링하십시오.

- 구성 요소 일련 번호를 사용하여 시스템 자산을 추적할 수 있습니다. Oracle 부품 번호는 모든 카드, 모듈 및 마더보드에 전자적으로 기록되어 있습니다.

보안 환경 계획

서버 및 Oracle Storage 12Gb/s SAS PCIe RAID HBA, 내부를 설치 및 구성하기 전이나 설치 및 구성하는 동안 이 절의 내용을 검토하십시오.

이 절은 다음 항목으로 구성됩니다.

- “하드웨어 보안” [7]
- “소프트웨어 보안” [7]
- “펌웨어 보안” [8]
- “Oracle ILOM 펌웨어” [8]
- “시스템 로그” [8]

하드웨어 보안

물리적 하드웨어는 하드웨어에 대한 액세스 제한 및 일련 번호 기록을 통해 매우 간단하게 보안을 설정할 수 있습니다.

- 액세스 제한
 - 잠금 문이 있는 랙에 장비가 설치된 경우 랙의 구성 요소를 수리해야 하는 경우를 제외하고는 문을 잠가 둡니다.
 - 예비 FRU(현장 교체 가능 장치) 또는 CRU(자가 교체 가능 장치)는 잠긴 캐비닛에 보관합니다. 권한이 부여된 담당자만 잠긴 캐비닛에 접근할 수 있도록 제한합니다.
- 일련 번호 기록
 - 모든 HBA 카드의 일련 번호를 기록해 둡니다.

소프트웨어 보안

소프트웨어 구성 요소에 대한 보안 고려 사항은 다음과 같습니다.

- 소프트웨어에 사용 가능한 보안 기능을 사용으로 설정하려면 소프트웨어와 함께 제공된 설명서를 참조하십시오.
- HBA 드라이버를 설치하고 업데이트할 때는 슈퍼 유저 계정을 사용합니다.
- 대부분의 하드웨어 보안은 소프트웨어 수단을 통해 구현됩니다.
- HBA를 지원하는 소프트웨어 구성 요소는 시스템 보안 기능을 사용하여 보안 액세스를 제공합니다.

펌웨어 보안

HBA는 모든 펌웨어가 설치된 상태로 제공됩니다. 따라서 업데이트하는 경우가 아니라면 펌웨어를 설치할 필요는 없습니다.

- 펌웨어 업데이트가 필요한 경우 펌웨어 업데이트는 LSI 웹 사이트의 Oracle 지원 영역 (<http://www.lsi.com/sep/Pages/oracle/index.aspx>)에서 구합니다.
오라클 고객 지원 센터에 문의하여 지원을 요청하거나 제품에 대한 최신 업데이트 및 절차를 확인할 수도 있습니다.
<https://support.oracle.com>
- HBA 펌웨어 관리 유틸리티를 설치하고 업데이트할 때는 슈퍼 유저 계정을 사용합니다. 일반 사용자 계정을 사용하면 펌웨어를 볼 수는 있지만 편집할 수 없습니다. Oracle Solaris OS 펌웨어 업데이트 프로세스에서는 권한이 없는 사용자가 펌웨어를 수정할 수 없습니다.
- 최신 뉴스, 펌웨어 업데이트 요구 사항에 대한 정보 또는 기타 보안 정보는 Oracle 웹 사이트에 있는 HBA 설치 설명서를 참조하십시오.
- SPARC OBP(OpenBootPROM) 보안 변수 설정에 대한 정보는 *OpenBoot 4.x Command Reference Manual*을 참조하십시오.

Oracle ILOM 펌웨어

일부 x86 서버에 사전 설치된 Oracle ILOM(Integrated Lights Out Manager) 펌웨어를 사용하여 적극적으로 시스템 구성 요소를 보안, 관리 및 모니터링할 수 있습니다. 암호 설정, 사용자 관리 및 SSH(보안 셸), SSL(Secure Socket Layer), RADIUS 인증을 비롯한 보안 관련 기능을 적용할 때 이 펌웨어 사용에 대해 좀 더 자세하게 이해하려면 다음 Oracle ILOM 설명서를 참조하십시오.

<http://www.oracle.com/pls/topic/lookup?ctx=ilom31>

시스템 로그

- 로깅을 사용으로 설정하고 전용 보안 로그 호스트로 로그를 보냅니다.
- NTP 및 시간 기록을 사용하여 정확한 시간 정보가 포함되도록 로깅을 구성합니다.

보안 환경 유지 관리

HBA의 초기 설치 및 설정 후 계속해서 Oracle 하드웨어 및 소프트웨어 보안 기능을 사용하여 하드웨어를 제어하고 시스템 자산을 추적할 수 있습니다.

다음 절로 구성됩니다.

- “자산 추적” [9]
- “펌웨어 업데이트” [9]
- “소프트웨어 업데이트” [9]
- “로그 보안” [10]
- “모듈 보안” [10]

자산 추적

일련 번호를 사용하여 인벤토리를 추적할 수 있습니다. Oracle은 옵션 카드 및 시스템 마더 보드의 펌웨어에 일련 번호를 포함합니다. LAN 연결을 통해 이러한 일련 번호를 확인할 수 있습니다.

또한 무선 RFID(Radio Frequency Identification) 판독기를 사용하여 자산 추적을 추가로 간소화할 수 있습니다. Oracle 백서 *How to Track Your Oracle Sun System Assets by Using RFID*를 참조하십시오.

펌웨어 업데이트

장비에서 펌웨어 버전을 최신 상태로 유지합니다.

- 정기적으로 업데이트를 확인합니다.
- 운영 체제들이 대개 그렇지만 특히 Oracle Solaris에서는 카드를 관리하거나 드라이버 또는 펌웨어를 업그레이드하려면 루트 자격 증명으로 로그인해야 합니다.
- 항상 펌웨어의 최신 릴리스 버전을 설치합니다.

소프트웨어 업데이트

장비에서 소프트웨어 버전을 최신 상태로 유지합니다.

- Oracle Solaris 드라이버에 대한 소프트웨어 업데이트는 Oracle Solaris 패치 및 업데이트를 통해 제공됩니다.
- 다른 운영 체제 드라이버의 소프트웨어 업데이트는 <http://www.lsi.com/sep/Pages/oracle/index.aspx>에서 찾아볼 수 있습니다.
- 최신 뉴스, 소프트웨어 업데이트 요구 사항에 대한 정보 또는 기타 보안 정보는 Oracle 웹 사이트에 있는 HBA 설명서를 참조하십시오.
- 항상 소프트웨어의 최신 릴리스 버전을 설치합니다.
- 소프트웨어에 필요한 보안 패치를 설치합니다.
- 장치에는 펌웨어가 포함되어 있으며 펌웨어 업데이트가 필요할 수도 있습니다.

로그 보안

정기적으로 로그 파일을 검사하고 유지 관리하십시오.

- 발생 가능한 문제에 대비하여 로그를 검토하고 보안 정책에 따라 아카이브합니다.
- 로그 파일이 적당한 크기를 초과할 경우 주기적으로 로그 파일을 처분합니다. 나중에 참조하거나 통계 분석에 사용할 수 있도록 처분할 파일의 복사본을 유지 관리합니다.

모듈 보안

HBA는 LSI StorCLI CLI(명령줄 인터페이스) 또는 MegaRAID SAS GUI(그래픽 사용자 인터페이스) 소프트웨어로 관리됩니다. 이 소프트웨어를 사용하여 다음을 수행할 수 있습니다.

- HBA 작업 모니터링
- HBA 펌웨어 업데이트

root 자격 증명을 사용하는 사용자만 StorCLI 및 MegaRAID SAS GUI 소프트웨어에 액세스할 수 있습니다. 따라서 권한이 없는 사용자는 이 유틸리티를 사용하여 SAN 환경을 변경할 수 없습니다.

StorCLI CLI 및 MegaRAID SAS GUI에 대한 자세한 내용은 웹 사이트(<http://www.lsi.com/sep/Pages/oracle/index.aspx>)에서 LSI 설명서를 참조하십시오.